REMARKS

Claims 28-41, 44, 45, 47, and 49-67 are currently pending in the subject application, and are presently under consideration. Claims 28-41, 44, 45, 47, and 49-67 are rejected. Claim 60 has been amended. Favorable reconsideration of the application is requested in view of the amendments and comments herein.

I. Rejection of Claims 28, 35, 41, 47, 53-56, and 58-66 Under 35 U.S.C. §103(a)

Claims 28, 35, 41, 47, 53-56, and 58-66 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,658,568 to Ginter, et al. ("Ginter") in view of U.S. Patent No. 6,816,900 to Vogel, et al. ("Vogel"), and further in view of U.S. Patent No. 6,233,341 to Riggins ("Riggins"). Claim 60 has been amended. Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claim 28 recites determining in the registration server that the user is entitled to the second certificate by ensuring that the user is still a member of the PKI enterprise and ensuring that the user does not already have the second certificate. The Office Action dated April 5, 2006 ("Office Action"), asserts that the claim element "ensuring that the user is still a member of the PKI enterprise" is taught by Vogel, and also asserts that the claim element "ensuring that the user does not already have the second certificate" is taught by Ginter (Office Action, page 3; citing Vogel, col. 1, ll. 26-40, and Ginter, col. 85, ll. 11-26). Representative for Applicant respectfully disagrees with both of these assertions.

Vogel teaches that Secure Sockets Layer (SSL) security protocol that utilizes a public key infrastructure (PKI) to maintain security (Vogel, col. 1, ll. 31-33). Vogel also teaches:

> In establishing an SSL connection between a client computer and a server computer hosting a web page, the server computer transmits a certificate to the client computer for verification. If a trusted certifying authority has approved the server computer (or web page) for secure connections, then a root certificate that is maintained at the client and issued by a root certifying authority (CA) will verify the certificate received from the server (Vogel, col. 1, ll. 33-40).

This section of Vogel, cited by the Examiner, merely discloses the establishment of an SSL connection by transfer and verification of a certificate from the server computer to the client computer. In neither this section of Vogel, as asserted by the Examiner, nor in any other section of Vogel does Vogel teach or suggest entitlement of a user to a second certificate by ensuring that the user is still a member of the PKI enterprise, as recited in claim 28. Thus, Representative for Applicant respectfully submits that the Examiner's reliance on Vogel to teach or suggest this element of claim 28 is misplaced.

Ginter teaches obtaining a certificate by submitting an identity certificate from a certifying authority to a different certifying authority that has a trusted database of people and/or organizations having a particular attribute (Ginter, col. 84, line 64 through col. 85, line 5). The identity information of the certificate is compared with the contents of the trusted database to allow issuance of the certificate without the user being physically present to obtain a certificate (Ginter, col. 85, ll. 11-23). This section of Ginter, cited by the Examiner, discloses that a certifying authority maintains a database that is trusted by other certifying authorities, thus allowing a user to obtain a certificate based on a certificate from another certifying authority. In neither this section of Ginter, as asserted by the Examiner, nor in any other section of Ginter does Ginter teach or suggest entitlement of a user to a second certificate by ensuring that the user does not already have the second certificate, as recited in claim 28. Thus, Representative for Applicant respectfully submits that the Examiner's reliance on Ginter to teach or suggest this element of claim 28 is likewise misplaced. Accordingly, neither Vogel nor Ginter, individually or in combination, teach or suggest determining in the registration server that the user is entitled to the second certificate by ensuring that the user is still a member of the PKI enterprise and ensuring that the user does not already have the second certificate, as recited in claim 28.

The Examiner cites Riggins for disclosing an authority for generating a private/public key pair, sending the private key to the user, and signing the public key. The addition of Riggins does not cure the above mentioned deficiencies of Ginter and Vogel to teach or suggest determining in the registration server that the user is entitled to the second certificate by ensuring that the user is still a member of the PKI enterprise and ensuring that the user does not already

have the second certificate, as recited in claim 28. Riggins teaches that a certifying authority verifies the identity and other information about a user, creates a signed certificate, and sends the signed certificate to the user (Riggins, col. 1, ll. 40-67). Therefore, Riggins teaches only that the certifying authority signs the public key (Riggins, col. 1, ll. 59-67). However, Riggins does not teach or suggest sending the public key from the authority to another authority to be signed, as recited in claim 28. Therefore, Ginter, Riggins, and Vogel, individually or in combination, do not teach or suggest the elements of claim 28. Withdrawal of the rejection of claim 28, as well as claims 29-34 and 53-56 which depend therefrom, is respectfully requested.

Claim 35 recites tracking a pedigree of a user's first certificate and accessing a registration web page having a level of security that is commensurate with the pedigree of the user's first certificate. Representative for Applicant respectfully submits that, in the rejection of claim 35, the Examiner has not addressed these claim elements of claim 35. However, Representative for Applicant notes that claims 55, 62, and 64, which have been addressed by the Examiner, are substantially similar to the above recited claim elements of claim 35. Thus, in the foregoing discussion of claim 35, Representative for Applicant addresses the Examiner's comments regarding the rejection of claims 55, 62, and 64.

The Examiner asserts that Ginter teaches tracking a pedigree of a user's first certificate and accessing a registration web page having a level of security that is commensurate with the pedigree of the user's first certificate (Office Action, page 5; citing Ginter, col. 30, ll. 29-39). Representative for Applicant respectfully disagrees. The cited section of Ginter teaches:

> Certifying authority may certify organizations and machines as well as people. For example, certifying authority could issue a certificate attesting to the fact that Stanford University is an accredited institution of higher learning, or that the ACME Transportation Company is a corporation in good standing and is authorized to transport hazardous materials. Certifying authority could also, for example, issue a certificate to a computer attesting to the fact that the computer has a certain level of security or is authorized to handle messages on behalf of a certain person or organization (Ginter, col. 30, ll. 29-39).

This section of Ginter describes that inanimate objects, and not just users, can be issued certificates that provide proof of the information asserted. The cited section of Ginter describes nothing about a pedigree of a certificate. Also, the citation of Ginter states that a certificate for a computer can establish a security level of the computer, and not a registration web page, as recited in claim 35. In addition, the citation of Ginter does not describe that the security level of the computer pertains to access to the computer by a user, and further does not describe that the security level is commensurate with a pedigree of a user's certificate. Therefore, in neither this section of Ginter, as asserted by the Examiner, nor in any other section of Ginter does Ginter teach or suggest tracking a pedigree of a user's first certificate and accessing a registration web page having a level of security that is commensurate with the pedigree of the user's first certificate, as recited in claim 35. Thus, Representative for Applicant respectfully submits that the Examiner's reliance on Ginter to teach or suggest this element of claim 35 is misplaced.

The addition of Vogel and Riggins does not cure the above mentioned deficiencies of Ginter to teach or suggest tracking a pedigree of a user's first certificate and accessing a registration web page having a level of security that is commensurate with the pedigree of the user's first certificate, as recited in claim 35. Therefore, Ginter, Riggins, and Vogel, individually or in combination, do not teach or suggest the elements of claim 35. Withdrawal of the rejection of claim 35, as well as claims 36-40 and 57-61 which depend therefrom, is respectfully requested.

Claim 41 recites a user server accessing a registration server using a signature certificate of the user to create a connection, and that upon the registration server determining that the user is entitled to a replacement certificate, revoking a certificate which the replacement certificate is replacing. Representative for Applicant respectfully submits that, in the rejection of claim 41, the Examiner has not addressed these claim elements, and further respectfully submits that none of the cited references teach or suggest a user server accessing a registration server using a signature certificate of the user to create a connection, and that upon the registration server determining that the user is entitled to a replacement certificate, revoking a certificate which the replacement certificate is replacing, as recited in claim 41. In addition, as described above

regarding claim 28, Riggins teaches only that the certifying authority signs the public key (Riggins, col. 1, ll. 59-67), and thus does not teach or suggest sending the public key from the authority to another authority to be signed, as recited in claim 41. Accordingly, withdrawal of the rejection of claim 41, as well as claims 44, 45, 62, and 63 which depend therefrom, is respectfully requested.

Claim 47 recites a user server accessing a registration server using a signature certificate of the user to create a connection. Similar to that described above regarding claim 41, Representative for Applicant respectfully submits that, in the rejection of claim 47, the Examiner has not addressed this claim element, and further respectfully submits that none of the cited references teach or suggest a user server accessing a registration server using a signature certificate of the user to create a connection.

Claim 47 also recites a secure data channel being disposed between the server platform and the user server and being encrypted using the signature certificate. Representative for Applicant respectfully submits that, in the rejection of claim 47, the Examiner has not addressed this claim element of claim 47. However, Representative for Applicant notes that claims 56, 61, and 63, which have been addressed by the Examiner, are substantially similar to the above recited claim element of claim 47. Thus, in the foregoing discussion of claim 47, Representative for Applicant addresses the Examiner's comments regarding the rejection of claims 56, 61, and 63.

The Examiner asserts that Vogel teaches a secure data channel that comprises encrypting a transmission between a registration server and the user server using the signature certificate (Office Action, page 5; citing Vogel, col. 1, ll. 26-40, the SSL). As stated above, Vogel teaches an SSL security protocol that utilizes a PKI to maintain security (Vogel, col. 1, ll. 31-33). Vogel also teaches:

> In establishing an SSL connection between a client computer and a server computer hosting a web page, the server computer transmits a certificate to the client computer for verification. If a trusted certifying authority has approved the server computer (or web page) for secure connections, then a root certificate that

> is maintained at the client and issued by a root certifying authority (CA) will verify the certificate received from the server (Vogel, col. 1, ll. 33-40).

This section of Vogel, cited by the Examiner, merely teaches creation of a secure transmission by transfer of a certificate from the server computer which is being accessed to the client computer. The cited section does not, however, pertain to encryption of a signature certificate. The Examiner seems to be unappreciative of the difference between a signature certificate, which is typically used to digitally sign a document for identity verification, and an encryption certificate, which is typically used to encrypt a document for secure transmission. Thus, according to the recitations of the Present Application, and as presented in claim 47, a user can automatically obtain another certificate, such as an encryption certificate, using a signature certificate to encrypt a secure data channel (see also, *e.g.*, Present Application, page 5, line 6 through page 6, line 19). Neither Vogel nor any other cited art, individually or in combination, teaches or suggests a secure data channel being disposed between the server platform and the user server and being encrypted using the signature certificate, as recited in claim 47. Withdrawal of the rejection of claim 47, as well as claims 49-52 and 64-67 which depend therefrom, is respectfully requested.

Claims 53 and 59 recite revoking the first certificate upon determining that the user is entitled to the second certificate, and claim 66 recites that the server platform revokes the signature certificate upon the server platform generating the second certificate. The Examiner asserts that Riggins teaches claims 53, 59, and 66 (Office Action, page 5; citing Riggins, Abstract; col. 3, ll. 14-28 and 43-56; col. 4, ll. 23-31 and 47-61). Representative for Applicant respectfully disagrees. Riggins teaches a system for installing temporary certificates for a user at a remote site (Riggins, col. 3, ll. 15-16). Riggins also teaches that the temporary certificates can be revoked upon the user leaving the remote site (Riggins, col. 3, ll. 17-19) and that a revocation list is maintained that contains information identifying revoked temporary certificates to prevent improper use of unexpired certificates (Riggins, col. 3, ll. 50-54). Riggins further teaches that temporary certificates are checked by an authorizing website to see if they have been revoked when they are reviewed for authenticity (Riggins, col. 4, ll. 28-31 and 57-60).

These sections of Riggins, cited by the Examiner, merely teach that the temporary certificates are revoked when the user leaves the remote site, and that revocation is determined when the temporary certificate is checked for authenticity. In neither of these cited sections, nor anywhere else, does Riggins teach or suggest that a first certificate is revoked upon a user's entitlement to a second certificate or upon generation of the second certificate. Therefore, neither Riggins nor any other cited art, individually or in combination, teaches or suggests revoking the first certificate upon determining that the user is entitled to the second certificate, as recited in claims 53 and 59, or that the server platform revokes the signature certificate upon the server platform generating the second certificate, as recited in claim 66. Withdrawal of the rejection of claims 53, 59, and 66 is respectfully requested.

Claim 60 has been amended to correct an antecedent error. Claims 54 and 60 depend from claims 53 and 59, respectively, and thus should be patentable over the cited art for the reasons stated above regarding claims 53 and 59. In addition, claims 54 and 60 recite signaling both the directory and the another authority (certificate authority) that the first certificate has been revoked. The Examiner cites the same sections of Riggins in the rejection of claims 54 and 60 as was cited in the rejection of claims 53 and 59. As stated above, the cited sections of Riggins teach that the temporary certificates are revoked when the user leaves the remote site, and that revocation is determined by an authorizing website when the temporary certificate is checked for authenticity (see Riggins, Abstract; col. 3, ll. 14-28 and 43-56; col. 4, ll. 23-31 and 47-61). Thus, Riggins teaches that the authorizing website checks for revocation from the revocation list, and is not signaled as to revocation of a certificate.

Even assuming *arguendo* that Riggins teaches signaling revocation of a certificate, Riggins does not teach signaling revocation of the certificate to both a directory and to an authority, such as a certificate authority, that is different from the authority that digitally signs the public key. Therefore, neither Riggins nor any other cited art, individually or in combination, teaches or suggests signaling both the directory and the another authority (certificate authority) that the first certificate has been revoked, as recited in claims 54 and 60, respectively. Withdrawal of the rejection of claims 54 and 60 is respectfully requested.

With regard to claims 55, 62, and 64, as stated above in the discussion of claim 35, neither Ginter nor any other cited art teaches or suggests accessing a registration server comprises tracking a pedigree of the user's first certificate to access a registration web page having a level of security that is commensurate with the pedigree of the user's first certificate, as recited in claims 55, 62, and 64. Withdrawal of the rejection of claims 55, 62, and 64 is respectfully requested.

With regard to claims 56, 61, and 63, as stated above in the discussion of claim 47, neither Vogel nor any other cited art teaches or suggests creating a secure data channel comprises encrypting a transmission between registration server and the user server using the signature certificate, as recited in claims 56, 61, and 63. Withdrawal of the rejection of claims 56, 61, and 63 is respectfully requested.

Claims 58 and 65 recite determining in the server platform that the user is entitled to the second certificate by ensuring that the user is still a member of the PKI enterprise and ensuring that the user does not already have the second certificate. The Examiner asserts that Vogel teaches claims 58 and 65 (Office Action, page 6; citing Vogel, col. 1, ll. 26-40). Representative for Applicant respectfully submits that, in the rejection of claim 28, the Examiner asserted that "determining in the server platform that the user is entitled to the second certificate by ensuring that the user does not already have the second certificate" is taught by Ginter. As stated above with regard to claim 28, Ginter does not teach or suggest determining in the server platform that the user is entitled to the second certificate by ensuring that the user does not already have the second certificate, as recited in claims 58 and 65. Furthermore, the section of Vogel cited in the rejection of claims 58 and 65 was also cited for the rejections of claims 28 and 47. As stated above, the cited section of Vogel merely discloses the establishment of an SSL connection in a PKI by transfer and verification of a certificate from the server computer to the client computer. However, as stated above regarding claim 28, neither Ginter nor Vogel, nor any other cited art, teaches or suggests determining in the server platform that the user is entitled to the second certificate by ensuring that the user is still a member of the PKI enterprise and ensuring that the

user does not already have the second certificate, as recited in claims 58 and 65. Withdrawal of the rejection of claims 58 and 65 is respectfully requested.

For the reasons described above, claims 28, 35, 41, 47, 53-56, and 58-66 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

II. Rejection of Claims 29, 57, and 67 Under 35 U.S.C. §103(a)

Claims 29, 57, and 67 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Ginter in view of Vogel in view of Riggins, and in further view of U.S. Patent No. 6,108,788 to Moses, et al. ("Moses"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 29, 57, and 67 depend from claims 28, 35, and 47, respectively, and are patentable for substantially the same reasons as claim 28 and for the specific elements recited therein. The addition of Haber does not cure the aforementioned deficiencies of Ginter, Vogel and Riggins to teach or suggest claims 28, 35, and 47, respectively. Accordingly, claims 29, 57, and 67 are patentable over the cited prior art.

III. Rejection of Claims 30-34, 36-40, 42-46, and 48-52 Under 35 U.S.C. §103(a)

Claims 30-34, 36-40, 42-46, and 48-52 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Ginter in view of Vogel in view of Riggins, and further in view of U.S. Patent 5,373,561 to Haber, et al. ("Haber"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 30-34 depend from claim 28 and are patentable for substantially the same reasons as claim 28 and for the specific elements recited therein. The addition of Haber does not cure the aforementioned deficiencies of Ginter, Vogel and Riggins to teach or suggest claim 28. Accordingly, claims 30-34 are patentable over the cited prior art.

Claims 36-40 depend from claim 35 and are patentable for substantially the same reasons as claim 35 and for the specific elements recited therein. The addition of Haber does not cure the

aforementioned deficiencies of Ginter, Vogel and Riggins to teach or suggest claim 28. Accordingly, claims 36-40 are patentable over the cited prior art.

Claims 42-46 depend from claim 41 and are patentable for substantially the same reasons as claim 41 and for the specific elements recited therein. The addition of Haber does not cure the aforementioned deficiencies of Ginter, Vogel and Riggins to teach or suggest claim 41. Accordingly, claims 42-46 are patentable over the cited prior art.

Claim 48-52 depend from claim 47 and are patentable for substantially the same reasons as claim 47 and for the specific elements recited therein. The addition of Haber does not cure the aforementioned deficiencies of Ginter, Vogel and Riggins to teach or suggest claim 47. Accordingly, claims 48-52 are patentable over the cited prior art.

CONCLUSION

In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date 6/26/06

Christopher P. Harris
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.
1300 EAST NINTH STREET, SUITE 1700
CLEVELAND, OHIO 44114
Phone: (216) 621-2234
Fax: (216) 621-4072